RENAISSANCE
ASSOCIATES, LTD.

PRIVILEGED AND CONFIDENTIAL

November 21, 2012

Ed Walton, Esq.
Bush & Ramirez, LLC
101 Metro Dr.
Terrell, Texas 75160

RE: Elisa Brooks-Cunningham and Courtney Douglas v. ER Solutions, Inc.

Dear Mr. Walton:

On November 12, 2012, I was engaged by Bush & Ramirez, LLC to render an opinion as to whether the disclosure of certain information in a mailing by ER Solutions, a collection agency, posed a threat of identity theft to the recipients.

In rendering this opinion, I relied upon my experience as an investigator and expertise in identity theft and fraud related matters, which includes the following:

I was a Special Agent in the FBI, New York Field Office, and the lead case agent on numerous high-profile investigations, including United States v. Cummings, a case that former United States Attorney for the Southern District of New York James Comey dubbed as the "largest identity theft case in United States history". Upon leaving the FBI, I continued to investigate complex white collar crimes for individuals and corporations, including those involving identity thefts.

I am a recognized expert in identity theft, having been interviewed by numerous media outlets and having been quoted in a variety of books and publications, including the New York Times among many others. I was named a "Thought Leader in Identity Theft Investigation" in the book, *Identity Theft Handbook, Detection, Prevention and Security* by Martin T. Biegelman, January 2009.

I am also a security consultant for the National Hockey League and the National Football League, and have co-written and hosted training videos for the National Hockey League, the National Football League and Major League Baseball on the topics of Identity Theft and Internet Security.

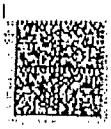
In the last ten years I have authored or co-authored the following articles: *To Catch a Thief*, New York Law Journal, May 30, 2006; *Truth Be Told, Successful Interviewing is an art*, New York Law Journal, May 29, 2007. I have not testified or been deposed within the past four years. My compensation for preparation of this report is $325 per hour. To date, the charges total $3,006.25.

Facts

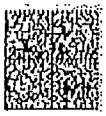
The facts, as told to me by Bush & Ramirez, LLC and as reflected in pleadings and answers to interrogatories, are as follows: The plaintiffs, Elisa Brooks-Cunningham (Brooks-Cunningham) and Courtney Douglas (Douglas) allege in their complaint that ER Solutions (a collection agency) sent to them collection notices in window envelopes. They further allege that through the window there was a "readable symbol that discloses, among other things: The identity of the debt collector, the consumers' account numbers, and even the alleged balances owed, in violation of an express statutory provision against disclosure of this private information". More specifically, the Plaintiffs allege that a Quick Response (QR) Code was visible through the envelope window, which, when read "with any popular device", "reveals the identity of the debt collector , ERS; the consumer's account number; the consumer's name and address; the amount of the alleged debt claimed due".

The collection letters were sent to collect on debts reportedly due to mobile phone carriers: For Brooks-Cunningham, the letter was to collect on a debt reportedly due to Verizon; for Douglas, the letter was to collect on a debt reportedly due to T-Mobile USA.

The information as it appeared in the plaintiffs' envelope windows is depicted below.



ATERSO01
PO Box 1022
Wixom MI 48393-1022
CHANGE SERVICE REQUESTED



ATERSO01
PO Box 1022
Wixom MI 48393-1022
CHANGE SERVICE REQUESTED

In answers to interrogatories, ER Solutions provided all of the information encoded within the QR Codes:

Interrogatory No. 5: Set forth, *verbatim*, everything that you allege is revealed by scanning, or otherwise reading, the QR Code on the "September 22, 2011 collection letter from ER Solutions, Inc. to Eliza Brooks-Cunningham" referred to in Plaintiff's Rule 26(a)(1) Initial Disclosures.

Answer: ATERSO01,#K#02B-22141870,Elisa Brooks,982 Anchor St,,Phila,PA, 191241036823,B290W,432.21

Interrogatory No. 6: Set forth, *verbatim*, everything that you allege is revealed by scanning, or otherwise reading, the QR Code on the " "May 16, 2011 collection letter from ER Solutions, Inc. to Courtney Douglass" referred to in Plaintiff's Rule 26(a)(1) Initial Disclosures.

Answer: ATERSO01,#K#02R-76305459,Courtney Douglass,228 King St Apt 3,, Pottstown,PA,194645515280,R241,802.04 (underlining in original)

I have reviewed the information contained in the decoded QR Codes above. I am completely unable to discern or decode any personally identifiable information from the numbers in the decoded information. The identity of ERS Solutions is not apparent (it is likely represented numerically and not in plain text) nor is the amount of the debt owed, as there are no dollar signs to signify currency anywhere in the decoded QR code. The "consumer's account" contained on the envelope and in the QR code is not identified as an account number and is an ER Solutions internal account number, not the account number for the underlying creditor (in this case Verizon and T-Mobile USA). Neither of the plaintiffs have been a victim of Identity Theft.

Discussion

Identity Theft is a crime in which someone wrongfully obtains and uses another person's personal information to commit a fraud. Identity Theft continues to be the fastest growing crime in America. The 2011 Identity Fraud Survey Report released by Javelin Strategy & Research found that in 2011 identity fraud increased by 13 percent. In 2011, more than 11.6 million adults became a victim of identity fraud in the United States[1]. It is widely accepted that the three key pieces of information that are essential to commit identity theft are a person's full name, date of birth and social security number. Of these three pieces of information, the social security number is by far the most important to an identity thief. Often referred to as the "golden key" to identity theft, knowing a person's social security number alone enables a thief to obtain a person's credit report and establish credit and open bank accounts and credit cards in that person's name.

With a social security number, a thief can easily obtain a vast amount of additional information about an individual, including full name, date of birth and address, among many others; however, having a date of birth, full name and/or address does not permit a thief to obtain an individual's social security number. There are numerous online services, both pay and free, which can be utilized to obtain publically available information about an individual. The publically available information generally consists of some or all of the following: Full name, date or month and year of birth, address history and relatives. Much of the information compiled by the online services is purchased in the form of credit header information from Credit Reporting Agencies, which are bound by the Gramm-Leach-Bliley (GLB) Safeguards Rule requiring reasonable protections for customers' sensitive personal and financial information. This protection includes not selling full social security numbers other than for law enforcement purposes. As such, complete social security numbers are not publically available or readily accessible.

Conclusion

The information contained in the QR codes on the mailings sent by ER Solutions to the plaintiffs does not pose a threat of Identity Theft. According to the plaintiffs, the only information contained in the QR code was each Plaintiff's name, address, the amount of the debt allegedly owed, ER Solution's name, and "consumer account information", which is an internal account number for ER Solutions. Of note, even when decoded, all of the information other than the plaintiffs' names and addresses are represented numerically and would not be apparent to an identity thief. Most importantly, the QR codes DID NOT contain the plaintiffs' social security numbers or even their dates of birth.

[1] https://www.javelinstrategy.com/news/1314/222/Identity-Fraud-Rose-13-Percent-in-2011-According-to-New-Javelin-Strategy-Research-Report/d,pressRoomDetail

It is common for commercial mailings to contain QR Codes which are visible on the exterior of envelopes. Whether or not a mailing contains a QR code, virtually all mailings identify the sender and the name and address of the addressee in plain view so that the Unites States Postal Service can facilitate the mailing and return deficient mailings to the sender if necessary. Obviously, the identity of an addressee and sender do not increase the risk of the addressee being victimized by an identity thief.

Likewise, neither the amount of a debt owed, even if decipherable, nor an internal account number for ER Solutions enhance the plaintiffs' risk of Identity Theft. ER Solutions is not a credit card company or financial institution. A thief knowing the amount of a debt and an account number for a debt collection agency poses no more risk of identity theft than merely having a name and address. If ER Solutions was a credit card company and the QR code revealed a credit card number, this would increase the risk of Identity Theft, giving a thief the ability to make fraudulent credit cards with the recipient's name and card number. In this case, however, a thief would merely have an internal file number for a collection agency which cannot reasonably lead to identity theft. Even if the thief was somehow able to obtain the underlying account numbers for Verizon and T-Mobile USA (and there is no evidence that this is the case), the thief would need to provide the mobile carriers with an account security code, social security number, or other personal identifying information before being able to access the accounts.

In sum, the Plaintiffs admit that a QR scanner would be necessary to view the information other than their names and addresses (which, as stated, is an integral part of every mailing). As reflected above, when the QR code is decoded the identity of ER Solutions and the amount of the debt are represented numerically and not obvious or apparent. Even if this information were apparent, it is of no value to an identity thief. Needless to say, unlike the mailings from ER Solutions, mailings from financial institutions, which clearly identify the sender as a financial institution and the recipient's name and address, are of much greater interest to an identity thief and pose an actual threat of identity theft if stolen.

Prepared By:

_____

Kevin Barrows
Managing Partner
Renaissance Associates, Ltd.